



Table of Contents

- **The need for Trusted Infrastructures**
- What is Trusted Computing?
- Leading the industry with the Trusted Computing Group
- Trusted Computing - Current State and Directions



The need for Trusted Infrastructures?

- Because we need security to be built-in across infrastructure components, not bolted-on after the facts
- Because we need to create an eco-system for trusted digital interactions
- With industry standard and certified security, if we are to successfully create a safer digital world



The need for Trusted Infrastructures

- Protect critical data in information systems
 - Data at rest or in transit
- Industry standard affordable security for mass-market systems
- Ubiquitous hardware root-of-trust for infrastructure security

Trusted Computing is a fundamental change that brings standard security building blocks to computing devices.



Table of Contents

- The need for Trusted Infrastructures
- **What is Trusted Computing?**
- Leading the industry with the Trusted Computing Group
- Trusted Computing - Current State and Directions



Trusted Computing Mechanisms

- Authenticate a platform
- Report integrity status of a platform
- Securely create/store/manage keys
- Protect platform against software attacks

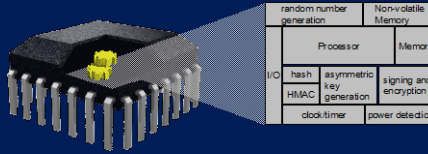
Trusted Computing helps establish that security mechanisms on computing device will behave as expected, for the intended purpose.



Trusted Computing Platforms Today

An embedded security chip for the protection of keys and secrets

HP ProtectTools
Vista BitLocker



And a brand-new value-proposition for IT... **device authentication**



TPM-based device authentication The VPN example

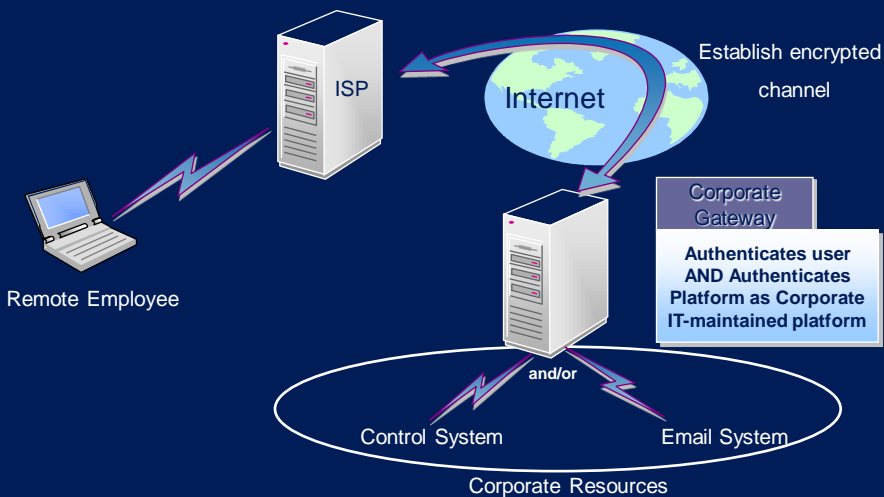


Table of Contents

- The need for Trusted Infrastructures
- What is Trusted Computing?
- **Leading the industry with the Trusted Computing Group**
- Trusted Computing - Current State and Directions



Trusted Computing & the Trusted Computing Group

**TRUSTED
COMPUTING GROUP™**

<http://www.trustedcomputinggroup.org>



Trusted Computing and HP

- HP was a founder of the Trusted Computing Platform Alliance (TCPA) in 1999, and again of the Trusted Computing Group (TCG) in 2003
- The TCG started its work from the specifications created by the TCPA organisation, and broadened its scope to more platform categories, from server to printers and mobile phones...
- Today the TCG has over 160 members, and its promoter members are AMD, HP, IBM, Infineon, Intel, Lenovo, Microsoft, and Sun.
- HP Labs holds the Technical Committee (TC) chair of TCG
 - HP chairs other technical working groups such as Hardcopy and Working Groups
 - HPLabs wrote the book on Trusted Computing Technology



Who is TCG?

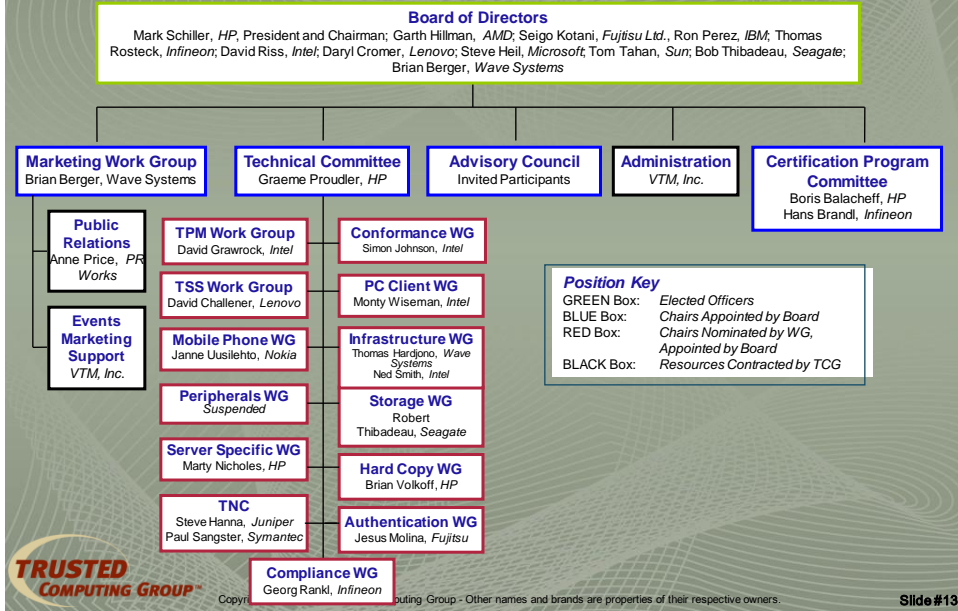
- The Trusted Computing Group (TCG) is an international industry standards group
- The TCG develops specifications amongst its members
 - Upon completion, the TCG publishes the specifications
 - Anyone may use the specifications once they are published
- The TCG publicizes the specifications and uses membership implementations as examples of the use of TCG Technology.
- The TCG is organized into a work group model whereby experts from each technology category can work together to develop the specifications
 - This fosters a neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable.



Copyright © 2005-2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Slide #12

TCG Organization

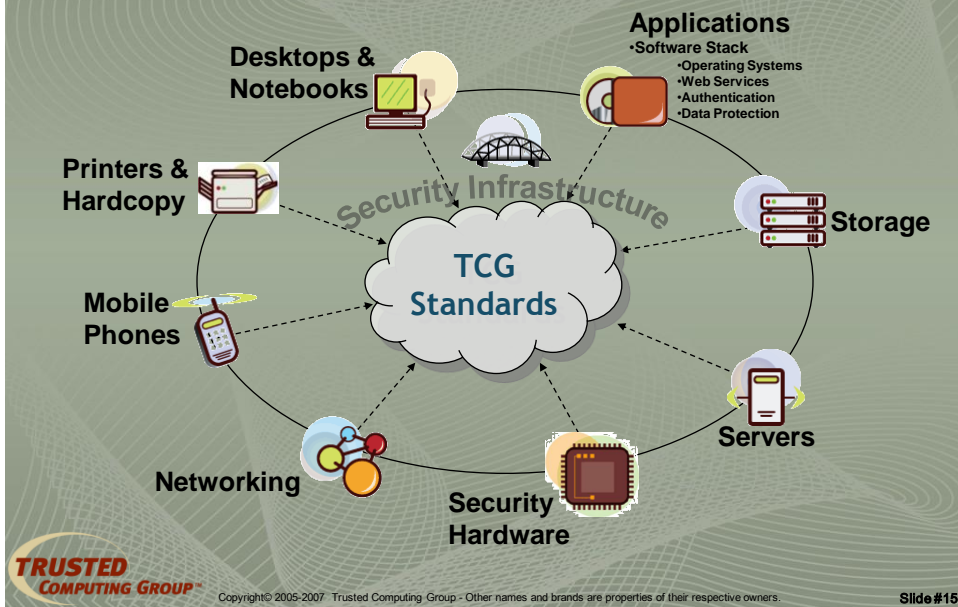


TCG Mission

Develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms

Standards drive Adoption

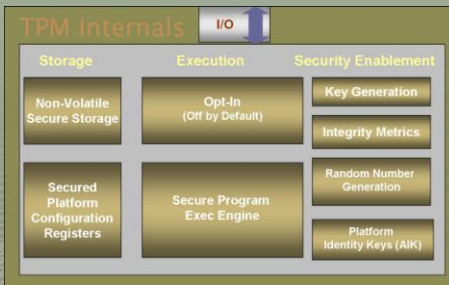
TCG: The "BIG" Picture



TPM – Key Features Summary

- Authenticate a platform
- Report integrity status of a platform
- Securely create/store/manage keys
- Protect itself against software attacks
- Fully controlled by the owner
 - Privacy positive implementation

Note: Contains no bulk encryption engine



TRUSTED COMPUTING GROUP™

Copyright © 2005-2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Slide #16

Table of Contents

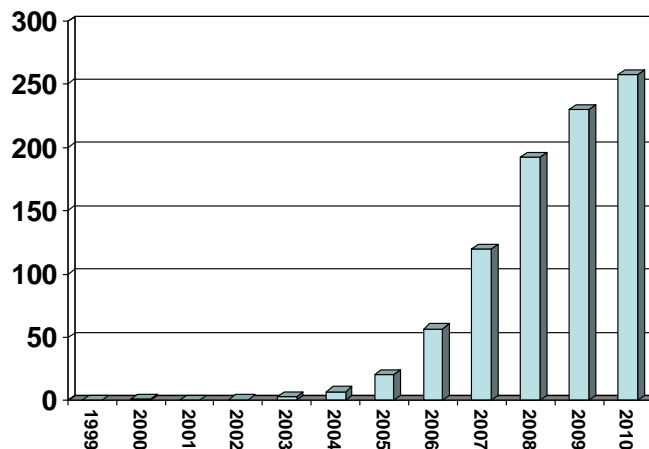
- The need for Trusted Infrastructures
- What is Trusted Computing?
- Leading the industry with the Trusted Computing Group
- **Trusted Computing - Current State and Directions**



TPM Module Forecast

IDC
Analyze the Future

(In millions of units shipped)



Source: IDC

Market Status Update

- TPM PCs – ~70 Million shipped through '06, > 100M estimated for 2007.
 - Most branded commercial notebook and desktop PCs have TPMs
- TPM servers available
- TPM providers –
- Trusted Network Connect (TNC) Products shipping
- Use cases released for mobile & storage capabilities
 - Storage proof of concept demonstration available
 - Draft specification for Mobile Trust Module
- Applications available and shipping with PCs & Servers



Copyright© 2005-2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Slide#19

Product Implementations

TPM Vendors:

Atmel
Broadcom
Infineon
Sinosun
STMicroelectronics
Winbond

Drive Makers

Seagate

Solutions for:

Data Protection
ID Management
Network Security
802.1X Security
VPN Security
SSO

TCG Solutions:

Infineon Professional Package
M-Systems
NTRU
Softex (Omni Pass and Theft Guard)
Utimaco (SafeGuard)
VeriSign (Personal Trust Agent)
Wave Systems (Embassy Trust Suites)

TNC Suppliers

Juniper
HP
Wave Systems

TCG Enabled PC Systems:

Dell (Latitude Notebook and Optiplex Desktop Series)
Fujitsu (LifeBook Notebook & Desktop systems)
HP (HP Protect Tools)
IBM (Embedded Systems Solution)
Intel (Intel® Desktop Board's – 12X)
Lenovo (T-Series)
Toshiba



Copyright© 2005-2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Slide#20

Some Examples



HP's Drive Lock

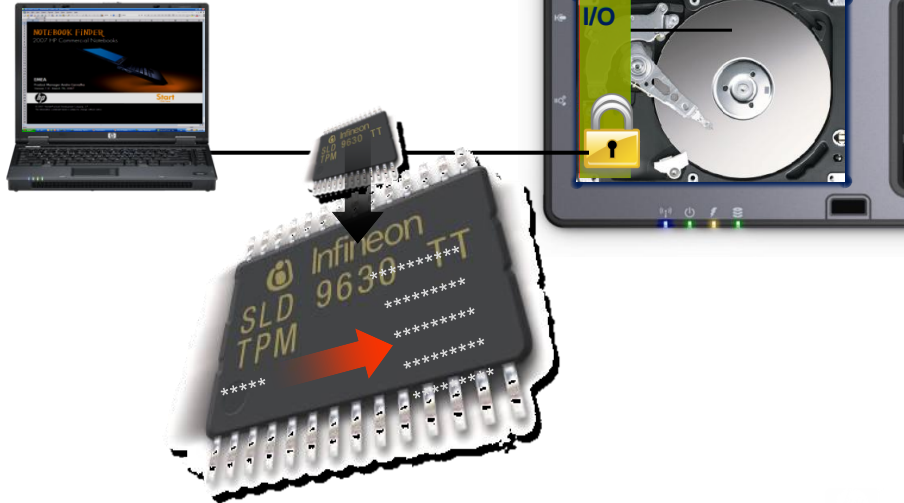
How does it work?



1. By setting up a BIOS User password, the Notebook is locked (the HDD does not allow any data to be accessed)
2. The Drive is now locked via BIOS password, restricting the access to the HDD.
3. If the user types the password...
 - ➕ The user can access the data.
 - ➖ Since BIOS passwords tend to be small (weak), they can be hacked, exposing the HDD data.
4. ...and the user can start his/hers applications.

HP Enhanced Drive Lock

How does it work?



Drive Encryption for HP ProtectTools

- Data Encryption is the best way to protect information on a hard drive
- HP includes Full Volume Encryption as a standard feature with most business notebooks
 - Safeboot technology
 - Windows XP & Vista support
 - broad authentication technology support –Smart Card, TPM and passwords
 - Single step login into Windows
- HP will include a single user version
 - Users can purchase Key backup and recovery subscriptions for convenient password recovery
 - Full enterprise capability available in partnership with Safeboot




Drive Encryption for HP ProtectTools

Full Volume Encryption How does it work?

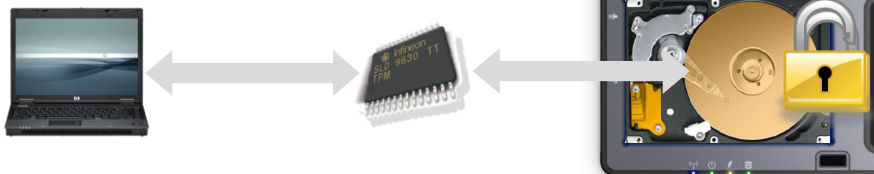


1. The user activates Full Volume Encryption and sets up a password.
2. The encryption key is protected by the TPM (If TPM is enabled)

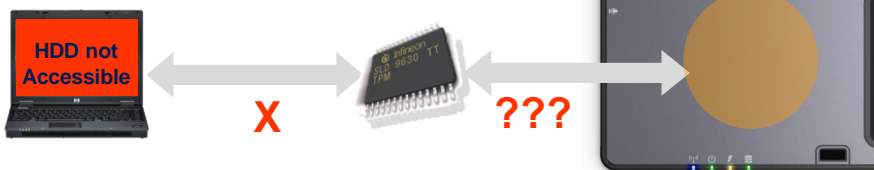
 The Data on the HDD is encrypted and even if the HDD is removed, the platters are placed in a different HDD, the Data is perfectly Secure.

Drive Encryption for HP ProtectTools

How does it work?

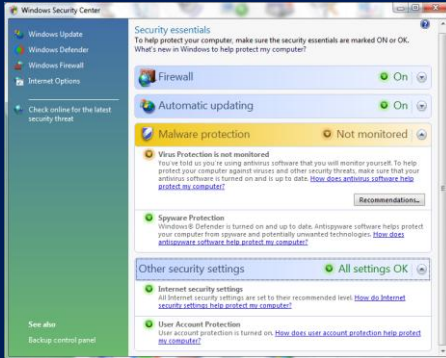


4. In case the Notebook is stolen, to access the data, the perpetrator may try to remove the HDD and put it into another Notebook.



Windows Vista BitLocker Drive Encryption

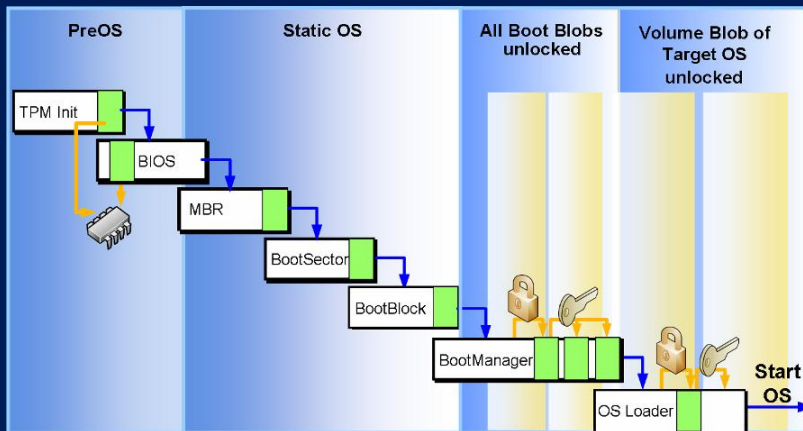
- Microsoft Windows Vista BitLocker security is ...
 - secure startup
 - full disk encryption
 - Ultimate & Enterprise only
 - requires TPM v1.2 hardware or external token
 - requires BIOS support
- all HP notebooks, desktops & workstations with TPM embedded security chips will support BitLocker



Windows Vista Security Center



Secure Startup Process



Trusted Computing status

- Trusted Platform Module (TPM) - the core of the TCG architecture
 - Available in client platforms today (i.e. HP business notebooks and desktops)
 - Data protection applications
 - Device authentication
 - Server availability emerging (i.e. HP Integrity server)
- Trusted Computing chain of trust implementations
 - Most business client systems
 - Used in Microsoft Vista BitLocker Drive Encryption™
- Enterprise solutions support
 - Management software solutions are emerging



Operating Systems Directions (near term)

- Expect increased Windows support
 - Server Support
 - Growing Client Support
 - Network Access Protection
- Expect increased Linux Support
 - Open Trusted Computing Effort
 - Commercial Distribution Support
- Expect increased support from UNIX derivatives
 - HP-UX, others



Operating Systems Directions (long term)

- Expect Virtualization Protection
- Expect Utility Data Center Protection



Hardware/Device Directions

- Expect Mobile Phones
- Increasing Mass Storage Uses
- Expect Network Infrastructure Device Applications
- Expect ubiquity in Commercial PCs
- Expect consumer use cases for PCs



Solution Directions

- Expect Network Access/Quarantine Applications
- Expect VPN Applications
- Expect end-to-end data protection applications
- Expect authentication and identity applications
- Expect hardcopy applications



Call to Action

- TCG needs members who will be users of the technology
 - To indicate market/application needs and requirements
- Users can't expect COTS equipment to satisfy their needs unless industry understands them



<https://www.trustedcomputinggroup.org/join/>

More on Trusted Computing in the HP Security Handbook

- Go to: www.hp.com/go/security



Questions?



